Quest

Quest® Migration Manager for Exchange 8.15

Source Exchange 2007 Environment Preparation

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Migration Manager for Exchange Source Exchange 2007 Environment Preparation
Updated - March 2020
Version - 8.15

Contents

Source Exchange 2007 Environment Preparation

Follow the steps that are described in the Preparation Checklist to prepare your Exchange 2007 organization and its environment for being the source organization in the Exchange migration process conducted by Migration Manager for Exchange.

On some of steps you may need to coordinate the setup process with the administrator of the target Exchange organization.

Preparation Overview

This section provides a short overview of the main steps that should be performed to set up your source Exchange 2007 organization and its environment for migration using Migration Manager for Exchange. These steps are described in detail below.

Setting up the source Exchange 2007 organization consists of four main steps:

Checking the System Requirements

On this step make sure that your environment meets the minimal system requirements for Migration Manager for Exchange agents. For more details, see Checking System Requirements.

Setting Up Accounts and Required Permissions

On this step you should set up the accounts and required permissions for Exchange migration. There are four main types of accounts used by Migration Manager for Exchange agents:

- Source Active Directory Synchronization Account
  This account is used by:
  a. The Directory Synchronization Agent (DSA) to access the source Active Directory domain
  b. The Mail Source Agent (MSA) to perform mailbox switch
- Source Exchange Account
  This account is used by Migration Manager for Exchange agents installed on agent host to access the source Exchange server.
- Source Active Directory Account
  This account is used by Migration Manager for Exchange agents to access the source domain.
- Source Agent Host Account
  This account is used to install and run the Migration Manager for Exchange agents on agent host and to access the license server.

You can simplify the setup by using a single account for all Migration Manager for Exchange processes. This account should have the permissions that are required for Migration Manager for Exchange console and all agents on every server that is involved in the migration.

For more details, see Setting Up Accounts and Required Permissions.

Preparing the Source Exchange Environment for Exchange Migration

On this step you should perform common environment preparations:

- Back up Exchange.
- Create the Aelita EMW Recycle Bin public folder (optional).
- Create administrator mailboxes for public folder and free/busy synchronization.
- Create administrator mailboxes for mailbox and calendar synchronization (optional).
- Install Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 version 6.5.8353.0 or later.
- Specify the displayName value for source Exchange 2007 mailbox database objects.

For more details, see Preparing the Source Exchange Environment for Exchange Migration.

Setting Up Connection with the Target Exchange Organization Using SMTP Connectors

On this step you should set up the connection with the target Exchange organization using SMTP connectors. This task consists of three subtasks given below:

1. Setting up the source Exchange 2007 organization for Internet mail flow between source and target Exchange organizations
2. Configuring the source DNS server for mail forwarding
3. Testing the SMTP connectors (optional)

For more details, see Setting Up Connection with the Target Exchange Organization Using SMTP Connectors.

Preparation Checklist

This checklist will help you set up your source Exchange 2007 organization and its environment properly. Make sure you have done all the steps below before completing the preparation.

Check	Step
□	Check the system requirements
□	Set up the Source Active Directory Synchronization Account
□	Set up the Source Exchange Account
□	Set up the Source Active Directory Account
□	Set up the Source Agent Host Account
□	Back up Exchange
□	Create the Aelita EMW Recycle Bin public folder (optional)
□	Create administrator mailboxes for public folder and free/busy synchronization
□	Create administrator mailboxes for mailbox and calendar synchronization (optional)
□	Install Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 version 6.5.8353.0 or later

Check	Step
□	Specify displayName value for mailbox database objects
□	Configure the NSPI connection limit
□	Set up the source Exchange 2007 organization for Internet mail flow between source and target Exchange organizations
□	Configure the source DNS server for mail forwarding
□	Test the SMTP connectors (optional)

Prerequisites

Before starting the preparation of the source Exchange 2007 organization and its environment, make sure that you have the privileges to grant all of the following permissions to accounts.

NOTE: The list of permissions given below contains all required permissions for the accounts. However some of the permissions can be replaced with their equivalents. For more information, see the corresponding steps for each account.

Source Active Directory Synchronization Account

- Membership in the **Administrators** or **Domain Admins** group of the source domain.

Source Exchange Account

- Membership in the local **Administrators** group on all source Exchange servers involved in the migration. If a server is a domain controller, the account should be added to the domain local **Administrators** group of the domain.
- **Full Control** permission on the organizational units (OUs) (and their child objects) where the source synchronized objects are located.
- **Full control** permission on source Exchange 2007 servers (including Send As and Receive As permissions).
- **Full Control** permission on the Microsoft Exchange System Objects organizational unit in all domains in which source Exchange 2007 servers involved in public folder synchronization reside.
- **Exchange Public Folder Administrator** role.

Source Active Directory Account

- **Read** access to the source domain.
- **Read** permission for the **Microsoft Exchange** container in the source Active Directory.

Source Agent Host Account

- Membership in the local **Administrators** group on the license server (unless alternative credentials are used for the license server). If server is located in another trusted forest, the account should have local Administrator permissions on the license server.
- Local **Administrator** permissions on the agent host server.

Checking System Requirements

> **CAUTION: Any computer that does not meet the requirements should be upgraded before installing Migration Manager for Exchange components.**

Migration Manager for Exchange uses the following Exchange-specific agents involved in the migration process:

- Public Folder Source Agent
- Public Folder Target Agent
- Mail Source Agent
- Calendar Synchronization Agent
- Free/Busy Synchronization Agent
- Transmission Agent
- Migration Agent for Exchange

Agents work on agent host servers.

Agent host can be:

1. An Exchange server itself, which is the default configuration. After you enumerate an Exchange organization all Exchange servers are registered as agent hosts for themselves.
2. Another Exchange server from the same Exchange organization.
3. A stand-alone server. It can be located in another forest or workgroup.

For detailed information about system requirements for agent hosts, see the *Exchange Migration Agents* section of the *System Requirements and Access Rights*.

Source Exchange 2007 Organization Considerations

- The mailbox database containing the administrator mailbox (the System Attendant mailbox used by default or custom administrator mailbox) should be mounted for each source Exchange 2007 server involved in the migration.
- The Migration Manager for Exchange console shows only those servers from source Exchange 2007 organization that host the Mailbox role. This is required because only servers with actual data are considered for migration.

Setting Up Accounts and Required Permissions

This section describes requirements for accounts working with the source Exchange servers. Migration Manager for Exchange allows you to use different administrative accounts for different purposes. Exchange data is migrated by Migration Manager for Exchange agents, which use the following accounts:

- Source Active Directory Synchronization Account
  This account is used by:
  a. The Directory Synchronization Agent (DSA) to access the source Active Directory domain

b. The Mail Source Agent (MSA) to perform mailbox switch

For more details, see Setting Up the Source Active Directory Synchronization Account for Exchange.

- Source Exchange Account
  This account is used by Migration Manager for Exchange agents installed on agent host to access the source Exchange server.
  For more details, see Setting Up the Source Exchange Account.
- Source Active Directory Account
  This account is used by Migration Manager for Exchange agents to access the source domain.
  For more details, see Setting Up the Source Active Directory Account.
- Source Agent Host Account
  This account is used to install and run the Migration Manager for Exchange agents on agent host and to access the license server.
  For more details, see Setting Up the Agent Host Account.

Setting Up the Source Active Directory Synchronization Account for Exchange

This section describes how to set the required permissions for the Source Active Directory Synchronization Account. This account is used by:

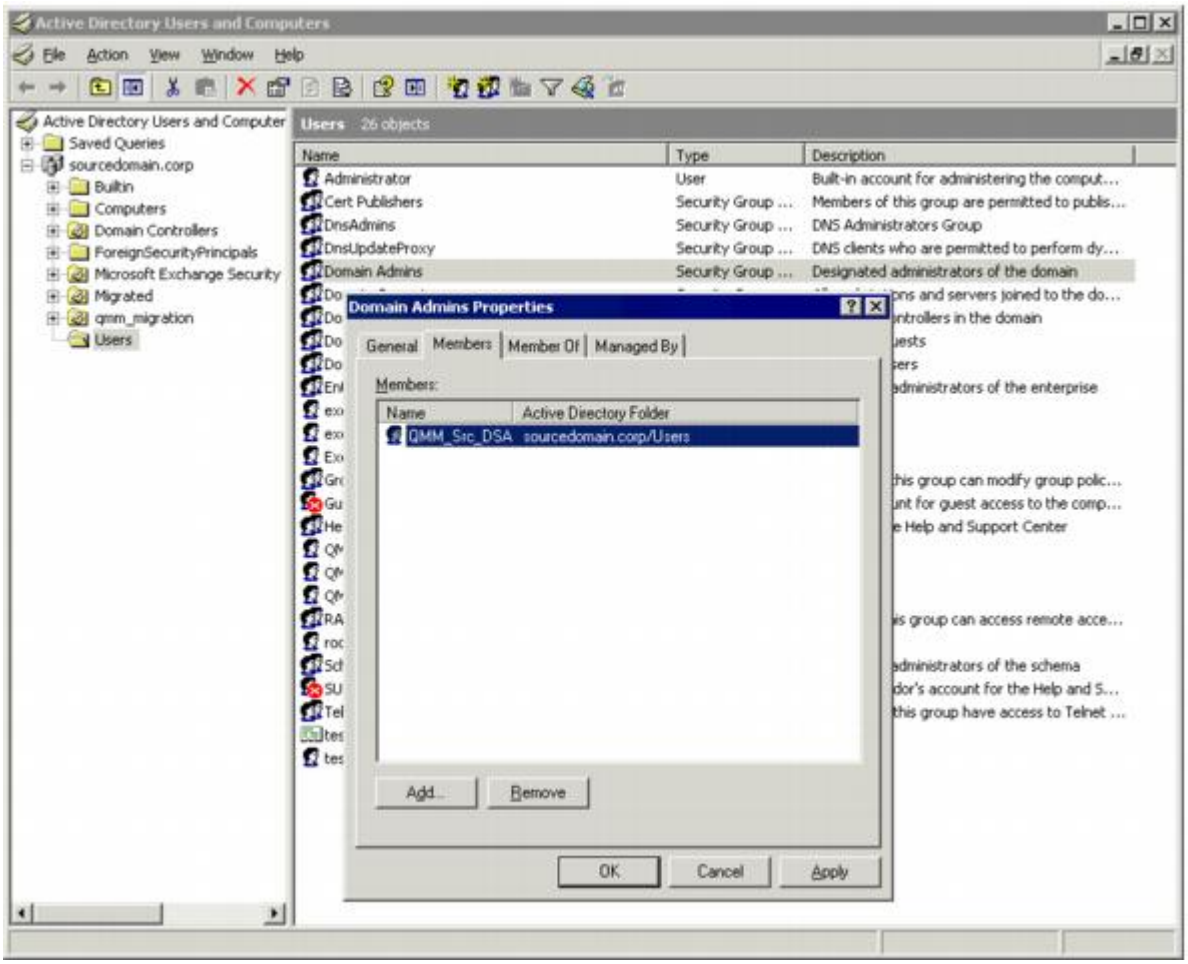
- The Directory Synchronization Agent (DSA) to access the source Active Directory domain
- The Mail Source Agent (MSA) to perform mailbox switch

The required privilege level for the Source Active Directory Synchronization Account is membership in the **Domain Admins** group of the source domain.

> **CAUTION: If for some reason you cannot grant such privileges to the Source Active Directory Synchronization Account, and then refer to the *System Requirements and Access Rights* document for the list of minimal required permissions.**

To grant the necessary permission to the Source Active Directory Synchronization Account, perform the following:

1. On the source domain controller in the **Active Directory Users and Computers** snap-in, click **Users**, then in the right pane right-click **Domain Admins** and click **Properties**.
2. Go to the **Members** tab, click **Add** and select the Source Active Directory Synchronization Account (in our example, **QMM_Src_DSA**).



3. Close the dialog boxes by clicking **OK**.

Setting Up the Source Exchange Account

This section describes how to set the required permissions for the Source Exchange Account used by Migration Manager for Exchange agents. This account is used for the following:

- Working with source Exchange mailboxes and public folders (used by the Mail Source Agent, Public Folder Source Agent, and Public Folder Target Agent)
- Making the newly-created public folders mail-enabled (used by the public folder agents only: Public Folder Source Agent and Public Folder Target Agent)
- Synchronizing Calendar information (used by the Calendar Synchronization Agent)
- Synchronizing free/busy data (optional) (used by the Free/Busy Synchronization Agent)
- Switching mailboxes

The required privileges for the Source Exchange Account are as follows:

- Membership in the local **Administrators** group on all source Exchange servers involved in the migration. If a server is a domain controller, the account should be added to the domain local **Administrators** group of the domain.
- **Full Control** permission on the organizational units (OUs) (and their child objects) where the source synchronized objects are located.
- **Full Control** permission on source Exchange 2007 servers (including the Send As and Receive As permissions).
- Full Control permission on the Microsoft Exchange System Objects organizational unit in all domains in which source Exchange 2007 servers involved in public folder synchronization reside.
- **Exchange Public Folder Administrator** role.

To set up the Source Exchange Account, perform the steps described in the related subtopics.

NOTE: Note that the steps are given only as an example of a possible Source Exchange Account setup.

Changing Default Exchange Account

The default Exchange Account (initially displayed on the **Connection** page of the Exchange server **Properties**) is set when you add the source or target organization to the migration project (see the *Registering Source and Target Organizations* section of the *Migration Manager for Exchange User Guide* for details). If necessary, you can change the default Exchange Account by clicking **Modify** on the **General** | **Connection** page in the properties of the corresponding server in the Migration Manager for Exchange Console.

Mailbox and calendar synchronization

The default Exchange Account for mailbox and calendar synchronization is specified when you create a corresponding synchronization job. To change it, use properties of the corresponding mailbox or calendar synchronization job.

Public folder synchronization

The default Exchange Account for public folder synchronization (initially displayed on the **Connection** page of the Exchange server **Properties**) is set when you add the source or target organization to the migration project (see the *Registering Source and Target Organizations* section of the *Migration Manager for Exchange User Guide* for details). If necessary, you can change the default Exchange Account for public folder synchronization by clicking **Modify** on the **General** | **Connection** page in the properties of the corresponding server in the Migration Manager for Exchange Console.

To go on using the default Exchange Account for Exchange migration, grant the permissions required for Exchange migration to this account (see the next steps).

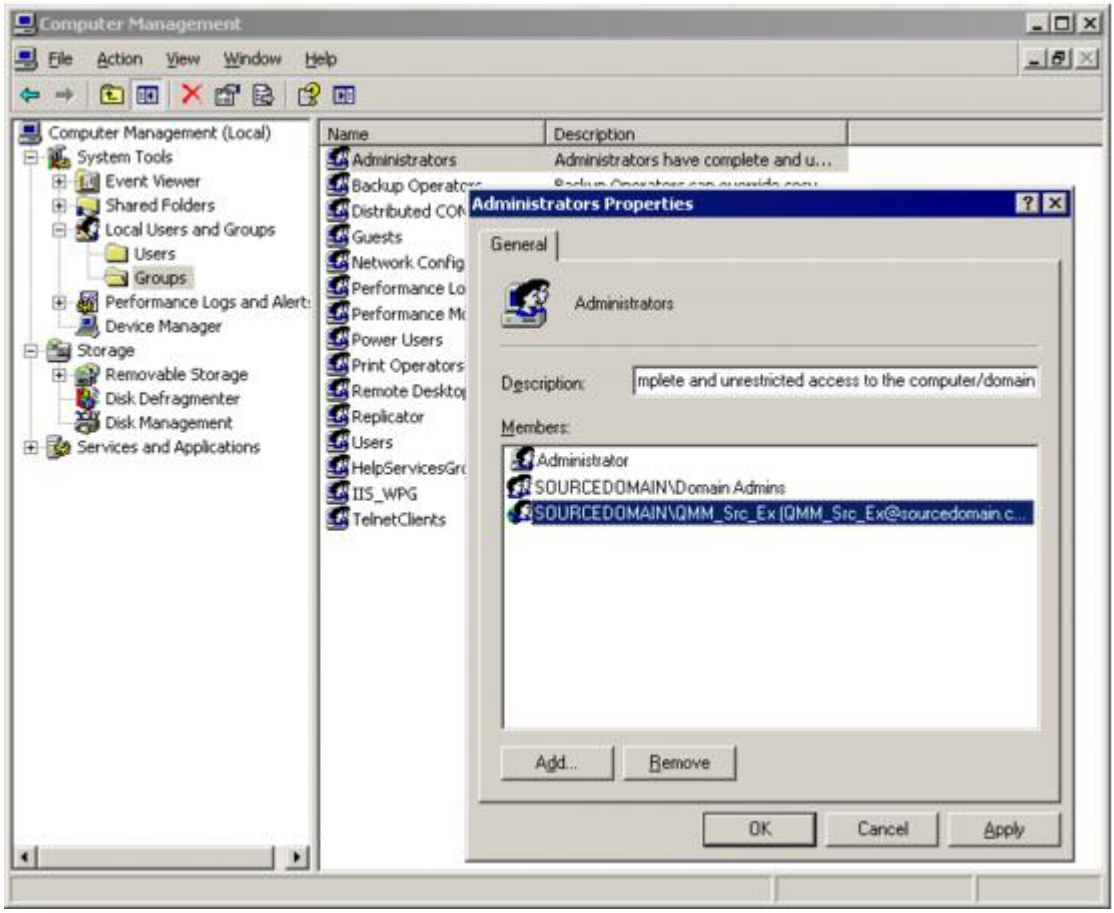
Granting Membership in Server Local Administrators Group

The Source Exchange Account used by Migration Manager for Exchange agents should be a member of the local **Administrators** group on each source Exchange server involved in the migration.

CAUTION: If the Exchange server is a domain controller, the account should be added to the domain local Administrators group of the domain.

To add the Source Exchange Account to the local **Administrators** group on each source Exchange server involved in the migration, perform the following:

1. Open the Computer Management snap-in (Click **Start** | **Run**, enter **compmgmt.msc** and then click **OK**).
2. In the left pane click **System Tools** | **Local Users and Groups** | **Groups**.
3. Right-click the **Administrators** group and click **Add to Group**.
4. Click **Add** and select the Source Exchange Account (in our example, **QMM_Src_Ex**).



5. Close the dialog boxes by clicking **OK**.

Granting Full Control on Organizational Unit

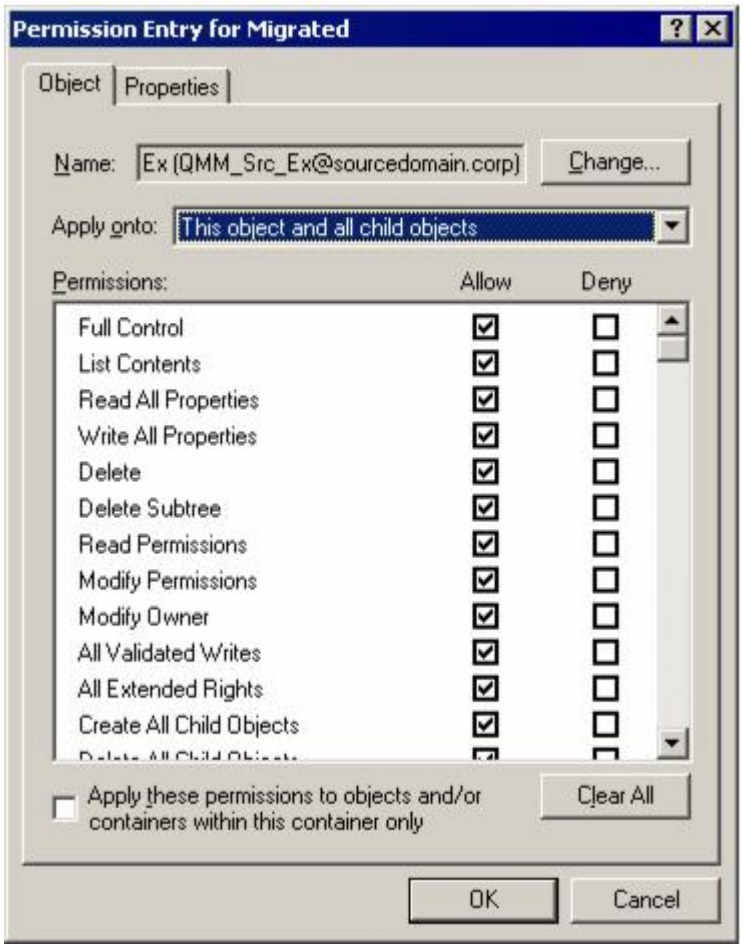
To work with the source Active Directory objects, the Source Exchange Account needs the **Full Control** permission on the organizational units and their child objects that contain the objects to be synchronized. This permission should be set on the domain controller where the objects you need to synchronize are located.

To grant the required permissions to the account, perform the following steps:

1. In the **Active Directory Users and Computers** snap-in, right-click the OU where the objects are located, and click **Properties**.
2. On the **Security** tab, click **Add**, and select the Source Exchange Account (in our example, **QMM_Src_Ex**).

> **NOTE:** If there is no **Security** tab, you should select **View | Advanced Features** in the **Active Directory Users and Computers** snap-in.

3. Select the account name, and then enable the **Allow** option for the **Full Control** permission in the **Permissions** box.
4. Click the **Advanced** button. In the **Advanced Security Settings** dialog box, select the account you specified on step 2, and click **Edit**.
5. 5 In the **Permission Entry** dialog box, select **This object and all child (descendant) objects** from the **Apply onto** drop-down list.



6. Close the dialog boxes by clicking **OK**.

Granting Full Control on Exchange Servers

The Source Exchange Account should have the Full Control permission on Exchange servers in the source Exchange 2007 organization, including the **Send As** and **Receive As** permissions.

To grant the required permissions to the account, do the following:

1. From the **Start** menu, select **Run**. In the **Run** dialog box, type **ADSIEdit.msc**. Click **OK**.

   NOTE: If you have a Windows 2003 domain controller, then the ADSIEdit utility, which is part of the Windows 2003 Support Tools, may not be installed. In this case install the Support Tools by running the **Support\Tools\Suptools.msi** file located on the Windows 2003 CD.

2. In the ADSIEdit snap-in, open the **CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<ExchangeOrganizationName>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<…>,DC=<…>** container.

For each Exchange server in this container that is involved in migration, complete the following steps:

a. Right-click the server object and select **Properties**.

b. In the **Properties** dialog box, click the **Security** tab.

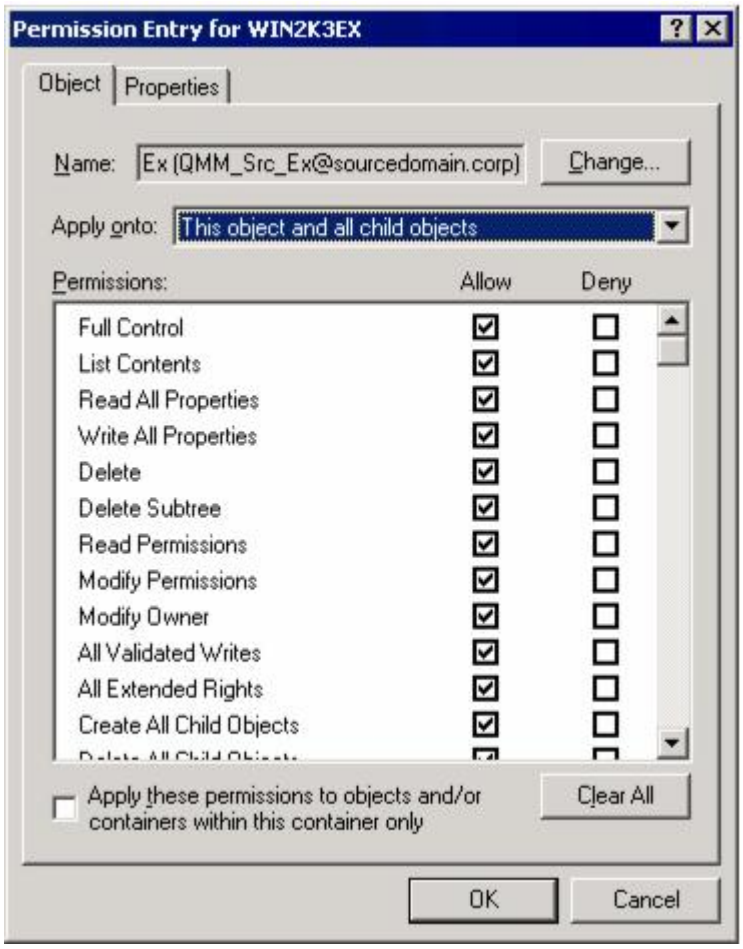
c. On the **Security** tab, click **Advanced**.

d. In the **Advanced Security Settings** dialog box, click **Add**.

e. In the **Select User**, **Computer**, or **Group** (or similar) dialog box, select the administrative account (in our example, **QMM_Scr_Ex**) and click **OK**.

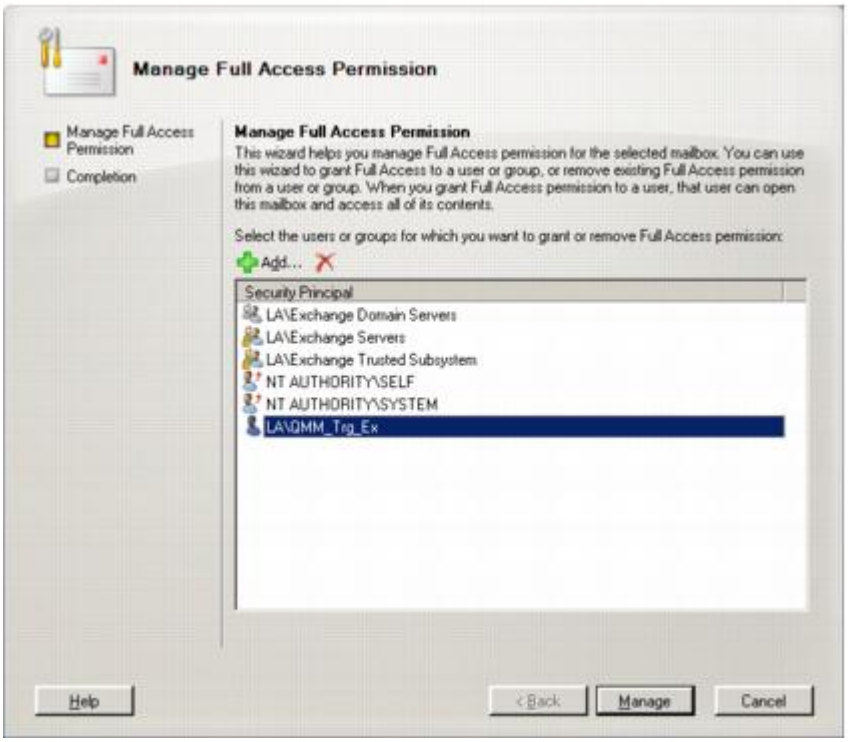
f. In the **Permission Entry** for dialog box, select **This object and all child (descendant) objects** from the Apply onto drop-down list.

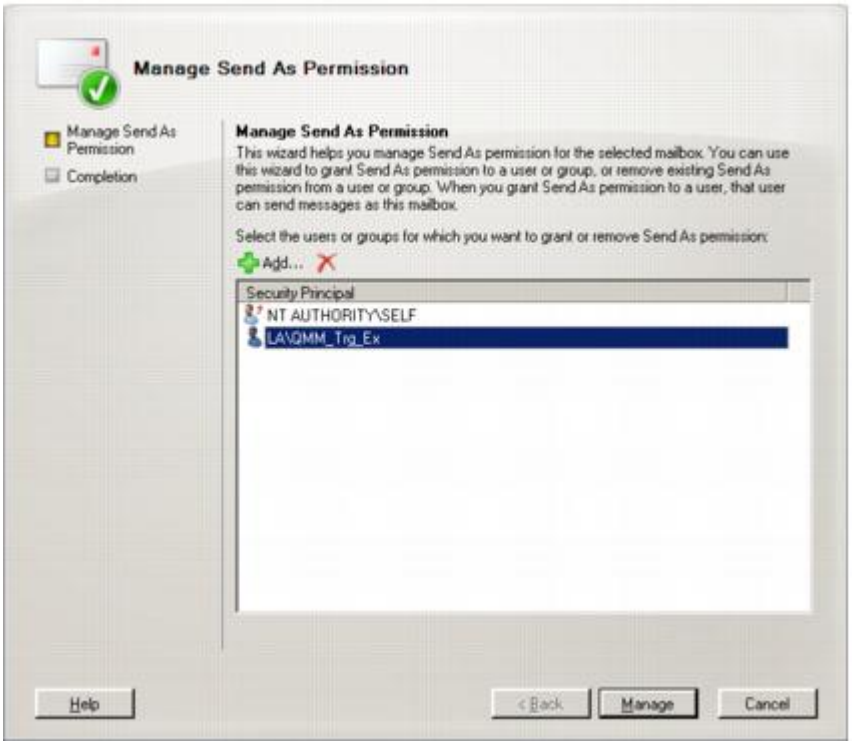
g. Allow **Full Control** permission for the administrative account, including the **Send As** and **Receive A**s permissions.



h. Close the dialog boxes by clicking **OK**.

To make sure the above actions were performed correctly, please view the **Manage Full Access** and **Manage Send As** dialogs in Exchange Management console. You should see the Source Exchange Account in both of the dialogs below.


Manage Full Access Permission
Manage Full Access Permission
Completion
Manage Full Access Permission
This wizard helps you manage Full Access permission for the selected mailbox. You can use this wizard to grant Full Access to a user or group, or remove existing Full Access permission from a user or group. When you grant Full Access permission to a user, that user can open this mailbox and access all of its contents.
Select the users or groups for which you want to grant or remove Full Access permission:
Add...
Security Principal
LA\Exchange Domain Servers
LA\Exchange Servers
LA\Exchange Trusted Subsystem
NT AUTHORITY\SELF
NT AUTHORITY\SYSTEM
LA\QMM_Trg_Ex
Help
< Back
Manage
Cancel


Manage Send As Permission
Manage Send As Permission
Completion
Manage Send As Permission
This wizard helps you manage Send As permission for the selected mailbox. You can use this wizard to grant Send As permission to a user or group, or remove existing Send As permission from a user or group. When you grant Send As permission to a user, that user can send messages as this mailbox.
Select the users or groups for which you want to grant or remove Send As permission:
Add...
Security Principal
NT AUTHORITY\SELF
LA\QMM_Trg_Ex
Help
< Back
Manage
Cancel

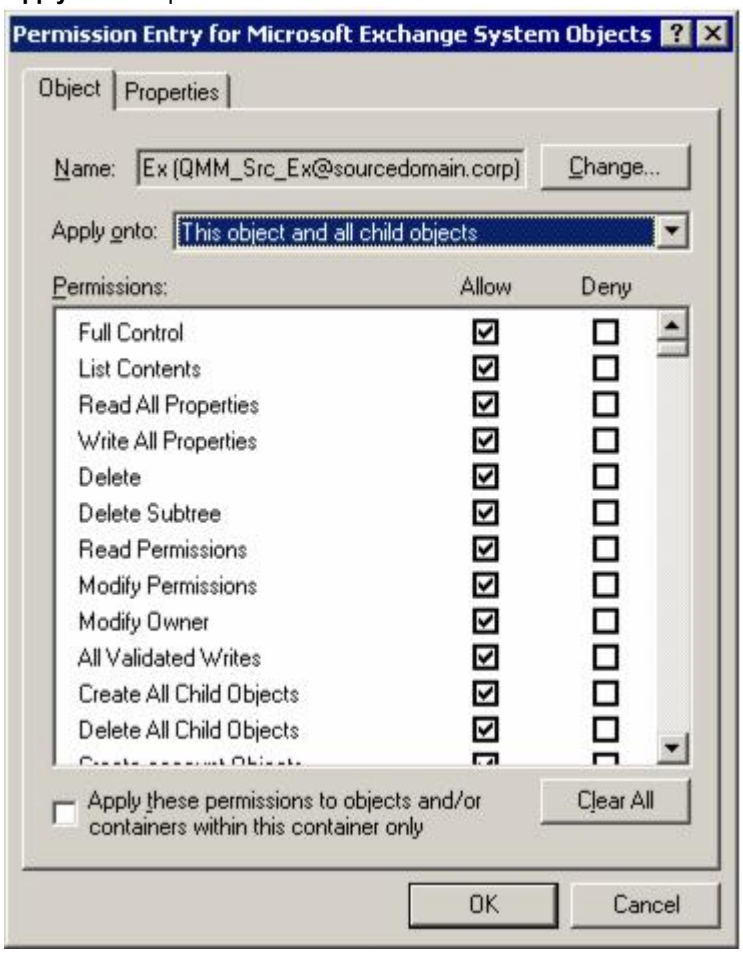
Granting Full Control on the Microsoft Exchange System Objects Organizational Unit

The Source Exchange Account used by Migration Manager for Exchange agents needs the Full Control permission on the Microsoft Exchange System Objects organizational unit (OU) in all domains in which source Exchange servers involved in public folder synchronization reside.

1. In the **Active Directory Users and Computers** snap-in, right-click the **Microsoft Exchange System Objects** OU and click **Properties**.

   NOTE: If there is no Microsoft Exchange System Objects OU, you should select View | Advanced Features in the Active Directory Users and Computers snap-in.

2. On the **Security** tab, click **Add**, and select the Source Exchange Account (in our example, **QMM_Src_Ex**).
3. Select the account name, and then enable the **Allow** option for the **Full Control** permission in the **Permissions** box.
4. Click the **Advanced** button. In the **Advanced Security Settings** dialog box, select the account you specified on step 2, and click **Edit**.
5. In the **Permission Entry** dialog box, select **This object and all child (descendant) object**s from the **Apply onto** drop-down list.



6. Close the dialog boxes by clicking **OK**.

Granting the Exchange Public Folder Administrator Role

The Source Exchange Account requires the **Exchange Public Folder Administrator role**.
To grant it, complete the following steps:

1. Launch the Exchange Management Console.
2. Click the **Organization Configuration** node. **Exchange Administrators** tab will appear in the right pane.
3. Right-click anywhere in the **Exchange Administrators** tab and select **Add Exchange Administrator** from the shortcut menu.
4. In the **Add Exchange Administrator** dialog box click **Browse**, select the Source Exchange Account (in our example, **QMM_Src_Ex**) and click **OK**.
5. Select the **Exchange Public Folder Administrator role** option and click **Add**.
6. Click **Finish** to exit the wizard and apply your changes.

CAUTION: If the Source Exchange Account is located in another trusted forest, you cannot assign the Exchange Public Folder Administrator role to this account. In this case grant the following permissions for the Exchange Administrative Group (FYDIBOHF23SPDLT) container and its child objects to the account in the Configuration partition using the ADSIEdit snap-in:

- **Modify public folder replica list permission**
- **Modify public folder deleted item retention permission**
- **Modify public folder quotas permission**

Setting Up the Source Active Directory Account

This section describes how to set the required permissions for the Source Active Directory Account used by Migration Manager for Exchange agents. This account is used for the following:

- Working with the source Active Directory

The required permissions for the Source Active Directory Account are as follows:

- **Read** access to the source domain
- **Read** permission for the **Microsoft Exchange** container in the source Active Directory

To set up the Source Active Directory Account, perform the steps described in the related subtopics.

NOTE: Note that these steps are given only as an example of a possible Source Active Directory Account setup.

Changing Default Active Directory Account

CAUTION: This section is relevant to the public folder synchronization only. Active Directory Account for mailbox or calendar synchronization is specified during corresponding job configuration.

The default Source or Target Active Directory Account (initially displayed on the Associated domain controller page of the Exchange server's properties) is set when you add the source or target organization to the migration project (see the *Registering Source and Target Organizations* section of the **Migration Manager for Exchange User Guide** for details).

To change the Source or Target Active Directory Account, click **Modify** on the **General | Associated domain controller** page of the corresponding source (target) server properties in the Migration Manager for Exchange Console.

To go on using the default Source (Target) Active Directory Account for Exchange migration, grant the permissions required for Exchange migration to this account (see the next steps).

Granting Read Access to Active Directory Domain

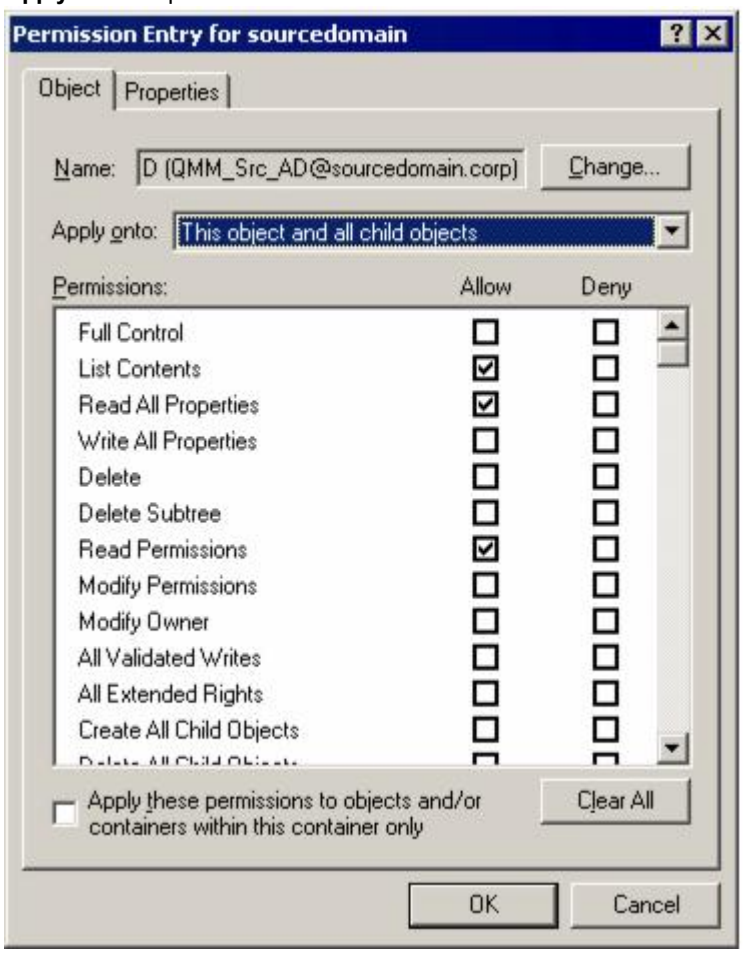
The Source Active Directory Account used by Migration Manager for Exchange agents needs **Read** access to the source domain to work with servers and source Active Directory.

To grant this permission to the account, complete the following steps:

1. On the source domain controller in the **Active Directory Users and Computers** snap-in, right-click the domain name, and then click **Properties** on the shortcut menu.
2. On the **Security** tab, click **Add** and select the account to which you wish to assign permissions (in our example, **QMM_Src_AD**).

   NOTE: If there is no **Security** tab, you should select **View** | **Advanced Features** in the **Active Directory Users and Computers** snap-in.

3. Select the account name, and then enable the **Allow** option for the **Read** permission in the **Permissions** box.
4. Click the **Advanced** button. In the **Advanced Security Settings** dialog box, select the account you specified on step 2 and click **Edit**.
5. In the **Permission Entry** dialog box, select **This object and all child (descendant) objects** from the **Apply onto** drop-down list.



6. Close the dialog boxes by clicking **OK**.

Granting Read Permission for the Microsoft Exchange Container

In the source Exchange 2007 organization, the Source Active Directory Account requires the **Read** permission on the **Microsoft Exchange** container in the source Active Directory.

To grant this permission to the account, complete the following steps:

1. Run the Exchange Management Console.
2. Click the **Organization Configuration** node. The **Exchange Administrators** tab will appear on the right pane.
3. Right-click anywhere in the **Exchange Administrators** tab and select **Add Exchange Administrator** from the shortcut menu.
4. In the **Add Exchange Administrator** dialog box click **Browse**, select the Source Active Directory Account (in our example, **QMM_Src_AD**) and click **OK**.
5. Select the **Exchange View-Only Administrator** role option and click **Add**.

6. Click **Finish** to exit the wizard and apply your changes.

CAUTION: If the Source Active Directory Account is located in another trusted forest, you cannot assign the Exchange View-Only Administrator role to this account. In this case grant the Read permission for the Microsoft Exchange container and its child objects to the account in the Configuration partition using the ADSIEdit snap-in.

Setting Up the Agent Host Account

This section describes how to set the required permissions for the Agent Host Account used by Migration Manager for Exchange agents. This account is used to install and run Migration Manager for Exchange agents on agent hosts and to access the license server. The required privileges for the Agent Host Account are as follows:

- Membership in the local **Administrators** group on the license server (unless alternative credentials are used for the license server). If server is located in another trusted forest, the account should have local **Administrator** permissions on the license server
- Local **Administrator** permissions on the agent host server.
- Permission to create, read and write SCP in domain where agent host resides. The SCP object is located in the **CN=Exchange Migration Project,CN=QmmEx,CN=Migration Manager,CN=Quest Software,CN=System,DC=eternity,DC=<...> ,DC=<...>** Active Directory container.
- The **db_owner** role on the SQL server where the database resides. Note that this permission is required if you use **Windows authentication** option for connecting to SQL Server.

NOTE: By default each Exchange server is an agent host for itself. If you use the default agent host then to simplify the account setup process, you can grant these permissions to the Exchange Account and use it instead of the Agent Host Account.

To set up the Agent Host Account, perform the steps described in the related subtopics.

NOTE: Note that the steps are given only as an example of a possible Agent Host Account setup.

Changing the Default Source Agent Host Account

The default Source Agents Host Account (initially displayed on the **Default Agent Host** page of the Exchange server **Properties**) is set when you add the source organization to migration project (see the *Registering Source and Target Organizations* section of the *Migration Manager for Exchange User Guide* for details).

If necessary, you can change the default Source Agent Host Account by clicking **Modify** on the **General** | **Default Agent Host** page of the corresponding source server properties in the Migration Manager for Exchange Console.

To go on using the default Source Agent Host Account for Exchange migration, grant the permissions required for Exchange migration to this account (see the next steps).

Granting Membership in the Local Administrators Group on the License Server

The Source Agent Host Account should be a member of the local Administrators group on the license server (unless alternative credentials are used for the license server).

CAUTION:

- **If license server is a domain controller, the account should be added to the domain local Administrators group of the domain.**
- **Local** Administrator **permissions are required on the license server if this license server is located in another trusted forest.**

To add the Source Agents Host Account to the local **Administrators** group on the license server perform the following:

1. Open the **Computer Management** snap-in (Click **Start** | **Run**, enter **compmgmt.msc** and then click **OK**).
2. In the left pane click **System Tools** | **Local Users and Groups** | **Groups**.
3. Right-click the **Administrators** group and click **Add to Group**.
4. Click **Add** and select the Source Agent Host Account (in our example, **QMM_Src_AH**).
5. Close the dialog boxes by clicking **OK**.

Preparing the Source Exchange Environment for Exchange Migration

Perform the steps described in the related subtopics to ensure that your Exchange environment is ready for migration:

- Backing Up Exchange
- Creating Aelita EMW Recycle Bin Public Folder (Optional)
- Creating Administrator Mailboxes for Public Folder and Free/Busy Synchronization
- Creating Administrator Mailboxes for Mailbox and Calendar Synchronization (Optional)
- Installing the Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1
- Specifying displayName Value for Source Exchange 2007 Mailbox Database Objects
- Configuring the NSPI Connection Limit

Backing Up Exchange

Before implementing Migration Manager for Exchange in your production environment, back up your Exchange infrastructure. We recommend that Active Directory data be backed up at least twice a day during migration.

Transaction Log File Cleanup

When Migration Manager for Exchange synchronizes mail, for every megabyte of data migrated from the source to the target, a transaction log file of equal size is generated on the target Exchange server. Exchange-aware backup applications purge the transaction logs after the backup completes. By the time the backup finishes, all logged transactions have already been applied to the store and backed up to tape, making log cleaning safe.

Large transaction logs that are generated during mailbox migration quickly occupy free disk space. To work around this problem, perform one of the following:

- If a full backup strategy is implemented in the organization or there is no backup strategy at all, then circular logging may be enabled for unattended log deletion.
- If an incremental or differential backup strategy is already implemented in the organization, then make sure that logs are cleared automatically when backup process is finished. Do not enable circular logging in this case.

Note also that Microsoft recommends turning OFF circular logging on the Exchange server. For more information, refer to Microsoft Knowledge Base article 147524: XADM: How Circular Logging Affects the Use of Transaction Logs.

Creating Aelita EMW Recycle Bin Public Folder (Optional)

> **CAUTION: If you skip this step, you must manually turn off using the Aelita EMW Recycle Bin folder during public folder synchronization (set the UseRecycleBin parameter to 0). See the Use Fine-Tuning the Agents section of the Migration Manager for Exchange User Guide for details.**

If you plan to perform public folder synchronization using Migration Manager Public Folder agents, you should create a special public folder called **Aelita EMW Recycle Bin.** Replicate this folder to all the public folder servers involved in the public folder synchronization process.

This folder will help prevent data loss in case of accidental public folder deletion. When a public folder is deleted in one of the environments, the public folder synchronization agents move the corresponding folder in the other environment to the **Aelita EMW Recycle Bin** folder, if it exists, instead of permanently deleting the folder. You can use this folder to check whether important information has been deleted, and restore any data deleted by mistake.

> **CAUTION: Only deleted public folders will be put into the Aelita EMW Recycle Bin. If you delete a message from a public folder, it will be destroyed permanently in both the Source and Target Exchange organizations.**

Creating Administrator Mailboxes for Public Folder and Free/Busy Synchronization

Administrator mailboxes should be created on all Exchange servers involved in public folder and free/busy synchronization. These mailboxes will be used to access the public folder tree and the Schedule+ Free/Busy folder when creating public folder and free/busy synchronization jobs.

The administrative mailbox selected for public folder synchronization should reside in a private mailbox database located on the same server as the public folder database. The mailbox database should be also associated with that public folder database. To set this association, in **Exchange Management Console** open properties of the mailbox database and specify the public database as **Default public folder database** on the **Client Settings** tab.

> **CAUTION:**
>
> - **The administrator mailbox specified for the synchronization job should not be changed during the synchronization process.**
> - **The administrator mailboxes should not be included in mailbox or calendar synchronization jobs.**

Creating Administrator Mailboxes for Mailbox and Calendar Synchronization (Optional)

Mailbox and calendar synchronization agents access the migrated mailboxes via the administrator mailbox. By default, the Microsoft System Attendant mailbox is used as the administrator mailbox on Exchange 2007 servers. However, in some cases it is necessary to create custom administrator mailboxes and use them instead of the Microsoft System Attendant mailbox.

Installing the Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1

Migration Manager needs version 6.5.8353.0 or later of Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 to be installed on the computers where Migration Manager agents will run (that is, Exchange 2007 and 2010 Servers and agent hosts only).

Since the MAPI CDO setup package is not available for distribution, you should download it from the Microsoft Web site. At the moment of the last document update, the download link is http://www.microsoft.com/en-us/download/details.aspx?id=42040.

After installing the API, restart the computer.

Specifying displayName Value for Source Exchange 2007 Mailbox Database Objects

Mailbox databases in Exchange 2007 organizations are created with blank **displayName** parameters. As a result, some agents may stop working. To resolve this issue, you have to specify the **displayName** values for the source Exchange 2007 mailbox databases. You can do it either manually, as described below, or using the **SetStoreDisplayName.js** script located in the **QMMEx Reskit\Scripts** folder on the Migration Manager for Exchange Installation CD. You must run the script after you install Migration Manager for Exchange.

To specify the displayName value for the source Exchange 2007 mailbox database objects

1. Launch the ADSIEdit utility from the Windows Support Tools: click **Start** | **Run** and type in **ADSIEdit.msc**. Click **OK**.

   > **NOTE:** If you have Windows 2003 domain controller the ADSIEdit utility, which is part of the Windows 2003 Support Tools may not be installed. In this case install the Support Tools by running the **Support\Tools\Suptools.msi** file located on the Windows 2003 CD.

2. In the ADSIEdit snap-in, browse to the container named

   CN=Exchange Administrative Group (FYDIBOHF23SPDLT),
   CN=Administrative Groups,CN=<ExchangeOrganizationName>,
   CN=Microsoft Exchange,CN=Services,CN=Configuration,
   DC=<…>,DC=<…>

3. For each Exchange 2007 server involved on the migration steps, open the container named

   CN=<StorageGroup>,CN=InformationStore,CN=<ServerName>,
   CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),
   CN=Administrative Groups,CN=<ExchangeOrganizationName>,
   CN=Microsoft Exchange,CN=Services,CN=Configuration,
   DC=<...>,DC=<...>
4. Then, for each mailbox database, right-click the database object and select **Properties** from the shortcut menu.
5. On the **Attribute Editor** tab, copy the **adminDisplayName** attribute value to the **displayName** attribute value and click **OK**.
6. Click **OK** to apply the settings and close the dialog box.

Configuring the NSPI Connection Limit

IMPORTANT: This step must be performed only if you have any Windows Server 2008 or later domain controllers acting as Global Catalog.

By default, the maximum number of simultaneous Name Service Provider Interface (NSPI) connections equals to 50 per user for Windows Server 2008 or later domain controllers. Therefore, to avoid possible issues related to exceeding that value, you may need to increase the NSPI connection limit on all Windows Server 2008 or later domain controllers acting as Global Catalog. The recommended limit value equals the number of agent instances working simultaneously multiplied by 5.

To change the default connection limit for a domain controller, take the following steps:

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Locate and then click the following registry subkey:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS`
3. Click the **Parameters** key.
4. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
5. Type **NSPI max sessions per user**, and then press **Enter**.
6. Double-click **NSPI max sessions per user**, type the appropriate maximum number of the NSPI connections, and then click **OK**.
7. Restart the computer or restart Active Directory Domain Services.

For additional information, see the following Microsoft Support articles:

- Error: "Trying to connect to Microsoft Exchange Server" results in MAPI_E_LOGON_FAILED
- NSPI connection to a Windows-based domain controller causes MAPI client applications to fail and returns a "MAPI_E_LOGON_FAILED" error message

Setting Up Connection with the Target Exchange Organization Using SMTP Connectors

This section describes how to set up a connection with the target Exchange organization using SMTP connectors. On this step you may need to coordinate with the administrator of the target Exchange organization to set up the connection properly.

For more details, see the related topics:

- Setting up Source Exchange Organization for Internet Mail Flow between Source and Target Exchange Organizations
- Configuring Source DNS Server for Mail Forwarding
- Testing the SMTP Connectors (Optional)

Setting up Source Exchange Organization for Internet Mail Flow between Source and Target Exchange Organizations

You need to establish Internet mail flow between the source and the target Exchange organizations. For that, one of the following methods can be used:

- Establishing Internet mail flow directly through a Hub Transport server.
- Establishing Internet mail flow through a subscribed Edge Transport server.

Establishing Internet Mail Flow Directly Through a Hub Transport Server

If you choose this option, you need to create an **Internet Send** connector and **Receive** connector on an Exchange 2007 Hub Transport server that can be directly reached through the Internet.

To establish mail flow to and from the Internet through a Hub Transport server, follow these steps:

1. Create a Send connector (to send email from source (target) Exchange 2007 organization to the Internet) on the Hub Transport server.
2. Modify the default Receive connector for the source (target) domain to accept anonymous e-mail from the Internet
3. Add the e-mail domain used for redirection to the list of accepted domains on the Hub Transport server.

Each step is explained in further detail in the related subtopics.

NOTE: For information about configuring Receive connectors in Exchange 2007 organization, refer to the following Microsoft Knowledge Base articles:

- How to Allow Anonymous Relay on a Receive Connector
- Creating a Receive Connector that Grants Anonymous Relay to Specific Source IP Addresses
- Configure the Receive Connector as Externally Secured

Creating Send Connector

To create a Send connector, you can use either Exchange Management Console or Exchange Management Shell.

To create a Send connector using Exchange Management Console

1. Open the Exchange Management Console. Select **Organization Configuration** | **Hub Transport**.
2. In the action pane, click **New Send Connector**. The **New SMTP Send Connector** wizard runs.
3. When prompted, in the **Name** field, type a unique name for the connector, for example, "**QMM Send Connector.**" From the **Select the intended use for this Send connector** drop-down list, select **Custom**, and then click **Next**.
4. On the **Address space** page, click **Add**. In the dialog box displayed, specify the address space you want to use for mail redirection from source to target (target to source) organization (for example, ***.target.local** or ***.source.local**), select the **Include all subdomains** option, click **OK** and then click **Next**.
5. On the **Network settings** page, select **Use Domain Name System (DNS) "MX" records to route mail automatically**. Select the **Use the External DNS Lookup settings on the transport server** option.
6. Next, on the **Source Server** page, click **Add**. In the dialog box displayed, select one or more **Hub Transport** servers in your organization, click **OK** and then click **Next**.
7. Finally, on the **New Connector** page, click **New**, and then on the **Completion** page, click **Finish**.

To create a Send connector using Exchange Management Shell

Run the following command for the source Exchange organization:

```
new-SendConnector -Name 'QMM Send Connector' -Usage 'Custom' -AddressSpaces
'SMTP:*.target.local;1' -IsScopedConnector $false -DNSRoutingEnabled $true -
UseExternalDNSServersEnabled $true -SourceTransportServers 'ServerName'
```

where:

- ***.target.local** is the address space you want to use for mail redirection from source to target organization.
- ServerName is the Hub Transport server name.

Run the following command for the target Exchange organization:

```
new-SendConnector -Name 'QMM Send Connector' -Usage 'Custom' -AddressSpaces
'SMTP:*.source.local;1' -IsScopedConnector $false -DNSRoutingEnabled $true -
UseExternalDNSServersEnabled $true -SourceTransportServers 'ServerName'
```

where:

- ***.source.local** is the address space you want to use for mail redirection from target to source organization.
- ServerName is the Hub Transport server name.

Modifying Default Receive Connector

To modify the default Receive connector for the source or target Exchange 2007/2010 organization to receive mail from the Internet, you can use either Exchange Management Console or Exchange Management Shell.

To modify the default Receive connector using Exchange Management Console

1. Run Exchange Management Console. Select the **Server Configuration | Hub Transport** node.
2. In the **Hub Transport** pane select the appropriate Hub Transport server.
3. On the **Receive Connectors** tab, select the **Default <Server Name>** connector. In the **Actions** pane, click **Properties** for this connector.
4. In **Default <Server Name> Properties** dialog box, open the **Permission Groups** tab.
5. Select **Anonymous Users** to add anonymous permissions.
6. Click **OK** to apply the settings.

To modify the default Receive connector using Exchange Management Shell

Run the following command:

```
Set-ReceiveConnector -PermissionGroups 'AnonymousUsers, ExchangeUsers,
ExchangeServers, ExchangeLegacyServers' -Identity 'ServerName\Default ServerName'
```

Where ServerName is the Hub Transport server name.

Adding E-mail Domain Used for Redirection to the List of Accepted Domains on Hub Transport Server

To add a new Accepted domain on a computer that has the Hub Transport server role installed, you can use either Exchange Management Console or Exchange Management Shell.

To add a domain to Accepted Domains list using Exchange Management Console

1. Run the Exchange Management Console and select the **Organization Configuration** | **Hub Transport** node.
2. In the **Actions** pane, click **New Accepted Domain**. This will start the **New Accepted Domain** wizard.
3. On the first page, provide the following information:
    - **Name**—Specify the accepted domain in the user interface, such as **source.local** (target.local).
    - **Accepted Domain**—Specify the SMTP namespace for which the Exchange organization will accept e-mail messages, such as ***.source.local** (***.target.local**).
4. Select the **Authoritative Domai**n. **E-mail is delivered to a recipient in this Exchange organization** option for the accepted domain type.
5. Click **New**.
6. On the **Completion** page, click **Finish**.

To add a domain to Accepted Domains list using Exchange Management Shell

Run the following command for the source Exchange organization:

```
new-AcceptedDomain -Name 'source.local' -DomainName '*.source.local' -DomainType
'Authoritative'
```

where ***.source.local** is the address space you want to use for mail redirection from the target to the source organization.

Run the following command the target Exchange organization:

```
new-AcceptedDomain -Name 'target.local' -DomainName '*.target.local' -DomainType
'Authoritative'
```

where ***.target.local** is the address space you want to use for mail redirection from the source to the target organization.

Establishing Internet Mail Flow through a Subscribed Edge Transport Server

The second option for establishing Internet mail flow between the target and the source Exchange organizations (or between the source and the target Exchange organizations) is to subscribe the **Edge Transport** server to an Active Directory site. The connectors that establish mail flow to the Internet are created automatically when you subscribe an Edge Transport server to an Active Directory site by using the Edge Subscription process.

Before you begin this procedure, verify that the following prerequisites are met:

- Authoritative domains are configured on the Hub Transport server.
- E-mail address policies are configured on the Hub Transport server.
- Network communications over the secure LDAP port 50636/TCP are enabled through the firewall separating your perimeter network from the Exchange organization.

To establish mail flow to and from the Internet through a subscribed Edge Transport server, follow these steps:

1. Export the Edge Subscription file from the Edge Transport server.
2. Import the Edge Subscription file on the Hub Transport server.
3. Force EdgeSync synchronization to begin on the Hub Transport server.

Each step is explained in further detail in the related subtopics.

Export the Edge Subscription file from the Edge Transport Server

1. Run the following command on the Edge Transport server, providing the complete file path of the Edge Subscription file that you are creating.
   ```
   New-EdgeSubscription -FileName "C:\EdgeSubscriptionInfo.xml"
   ```
2. Copy the resulting XML file to the Hub Transport server.

Import the Edge Subscription file on the Hub Transport Server

On the Hub Transport server, run the following command:

```
New-EdgeSubscription -filename "C:\EdgeSubscriptionInfo.xml" -
CreateInternetSendConnector $true -CreateInboundSendConnector $true -site "Site-Name"
```

Where Site-Name is the name of Active Directory site where the Hub Transport server is located.

Force EdgeSync Synchronization

To force EdgeSync synchronization, run the following command from the Exchange Management Shell on the Hub Transport server:

```
Start-EdgeSynchronization
```

Configuring Source DNS Server for Mail Forwarding

After you have completed setting up the source Exchange 2007/2010 organization for Internet mail flow between source and target Exchange organizations, you should also add the Mail Exchanger (MX) record for the source domain to the DNS server. This is necessary to forward the mail (redirected to the additional SMTP addresses added by the Directory Synchronization Agent) to the source Exchange 2007/2010 server.

We will use the following additional address space given as example on the steps above:

- *@source.local*—to redirect mail from target to source mailboxes. A secondary SMTP address will be added to each source mailbox by the Directory Synchronization Agent according to this template.

To set MX record for the source domain

1. In the DNS snap-in, connect to the source DNS server and browse to the **Forward Lookup Zones** container.
2. Right-click the **Forward Lookup Zones** and select **New Zone**.
3. In the New Zone wizard, select the Primary zone to be created.
4. Type local for the Zone name and complete the wizard.
5. Right-click the zone object local again, and click **New Mail Exchanger** on the shortcut menu.
6. In the **New Resource Record** dialog box, type source for the **Host or child domain**.
7. Click **Browse** and select the Exchange server in the source domain to which mail sent to the *@source.local* domain will be redirected.
8. Click **OK**.

Testing the SMTP Connectors (Optional)

After both source and target Exchange organizations have been set up for Internet mail flow as well as both source and target DNS servers have been configured for mail forwarding, it is recommended to test the connection between the source and the target organizations.

> **CAUTION: This step should be performed in coordination with the administrator of the Exchange organization.**

To test the SMTP connectors:

1. Create test mailboxes on the source and target Exchange servers. In this example, both mailboxes will be called **mbx1**.
2. Set the same primary SMTP address for both mailboxes.
3. In this example the primary address for both mailboxes will be **mbx1@Westland.Exchange.com**.
4. Set additional addresses for both mailboxes.
5. In this example additional address for the source mailbox will be **mbx1@source.local**, and **mbx1@target.local** for the target mailbox.
6. Create a contact on the source Exchange server and point it to the additional SMTP address of the target Exchange mailbox (**mbx1@target.local**).
7. Create a contact on the target Exchange server and point it to the additional SMTP address of the source mailbox (*mbx1@source.local*).
8. Open the test source mailbox and send a message to the source contact.
9. Open the test target mailbox and make sure that the message has arrived.
10. From the test target mailbox, send a message to the target contact, and make sure the e-mail has reached the source test mailbox.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product